

JKnight

UNITED STATES DISTRICT COURT

for the
Southern District of OhioFILED
RICHARD L. JACOB
CLERK OF COURT

2019 MAR 22 AM 11:46

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)212 HARBORVIEW DRIVE,
THORNVILLE, OHIO 43076

Case No.

2:19-mj-235

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A.

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. 922(g)(1)

Felon in possession of firearms or ammunition

26 USC 5861(d)

Prohibited Possession of Unregistered Firearm

18 USC 115(a)(1)(B)

Threats to Federal Official

The application is based on these facts:

See attached affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

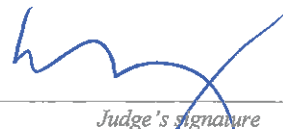
Jonathan Stierck Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: 3/22/19

City and state: Columbus, Ohio



Judge's signature

N. M. King, U.S. Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:
**212 HARBORVIEW DRIVE,
THORNVILLE, OHIO 43076**

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jonathan R. Stickel, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **212 Harborview Drive, Thornville, Ohio 43076**, hereinafter “PREMISES,” further described in Attachment A, for the things described in Attachment B.

2. I am a Task Force Officer (“TFO”) with the Federal Bureau of Investigation (“FBI”) Joint Terrorism Task Force (“JTTF”) and have been for two years. I am a Franklin County Deputy Sheriff Detective (OH) with twelve years of experience including four years of investigative assignments. I have specialized training related to narcotics investigations, crime scene processing, and domestic and international terrorism investigations. I have investigated or assisted with the investigation of multiple criminal violations, at both the Federal and State level, using a variety of investigative techniques, including grand jury subpoenas, search warrants, records analysis, consensual recordings, and undercover operations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

Background of Case

1. This case originated within the Federal Bureau of Investigation after reports of **SHADE** making comments and remarks of a threatening nature on social media via Twitter towards the President of the United States on multiple occasions and one directly towards a local United States Secret Service (USSS) agent. The tweet involving the local USSS agent came several weeks after the agent attempted a knock and talk at **SHADE'S** residence regarding a recent incident involving **SHADE** at an event involving the Vice President of The United States (VPOTUS). **SHADE** has a history of traveling within and out of state to attend political events as well as protests, and on several occasions, his conduct at these events has resulted in charges related to trespassing, obstructing, invasion of privacy and carrying weapons other than firearms (baton and pepper spray).

2. **SHADE** again came to the attention of the FBI on January 22nd, 2019 after an arrest and report from Cambridge Police Department.

3. Specifically, on January 21, 2019, a 911 call was received by dispatch of an unknown substance being thrown into a male's face causing the male to have trouble seeing. The caller was unsure if the suspect was still on the scene and advised that the male victim and two children were currently in the basement. Cambridge Fire and Police were dispatched to 539 Steubenville Ave, Cambridge Ohio 43725.

4. Upon arrival, Fire and Police advised there was a strong chemical odor and had the residents of the address H.D., B.M., D.M. and T.H. vacate the residence for safety. The male with symptoms, T.H., was taken to EMS to be evaluated.

5. Once cleared, H.D., B.M. and D.M. walked back into the residence with officers to look at the scene. Officers noted the chemical odor was still singing their nostrils. H.D. stated to officers they were all watching television and saw a flashlight. H.D. stated they went to the window to see what was outside and saw him just standing there, plain as day. H.D. stated all of the sudden he threw something through the window at T.H. Officers asked who the individual was and H.D. stated it was the landlord with the du-rag on, **JOHN SHADE**.

6. While officers were walking out of the garage next to where the incident occurred, they observed one set of footprints going from the back of 539 Steubenville Ave to the connected duplex of 541 Steubenville Ave.

7. Officers went to 541 Steubenville Ave and made contact at the front door. Four occupants were ordered outside, F.G, D.S., D.L. and **SHADE**. Officers noted that when **SHADE** came out of the residence, he was the only one with snow on his boots. The boots **SHADE** was wearing also matched the footprints in the rear of the residence going to and from 539 Steubenville Ave. Based on all information received from the witnesses, **SHADE** was placed under arrest. On **SHADE'S** person, among other items, were a flashlight, pepper spray, vehicle keys and cellphone. Officers also collected a Gerber baby food glass jar with an unknown substance inside that was thrown into the residence.

8. While officers spoke with F.G. outside he advised that he observed **SHADE** go downstairs for a period of time and then came back upstairs. When **SHADE** came back upstairs he told F.G. that the police might be coming.

9. T.H. was transported to the emergency room for evaluation of his injuries and symptoms. Officers went to the emergency room and spoke with T.H. who stated while he was at home he noticed a light flicker in his window. T.H. stated when he went to investigate he observed a male with a white bandana, dark jacket and grey beard through the window. T.H. stated he recognized the male as **SHADE**, his landlord, who then broke the window with a flashlight and threw a container at him which the contents burned his eyes.

Felon in Possession Investigation

10. On January 23, 2019, Cambridge Police officers executed a search warrant of **SHADE'S** 2011 Black GMC Terrain, which **SHADE** had driven to the scene of the incident, and located the following:

- One box of 9mm ammunition with purchase receipt
- Two pill bottles with various pills (IBProphen, Acetaminophen, Atorvastatin Calcium, Losartan Potassium and Sertraline Hydrochloride)
- Multiple press identifications
- Backpack containing multiple electronics and paperwork
- Water putty paste

11. Cambridge Police examined the receipt found inside a Walmart bag with the ammunition. The purchase was on January 8, 2019 at the Walmart located at 61205 Southgate

Road, Cambridge Ohio 43725. Cambridge Police obtained Walmart video surveillance footage and after review, officers identified **SHADE** making a cash purchase of the ammunition at the sporting goods counter. Specifically, **SHADE** purchased a Federal 9mm Luger FMJ-RN 100 round box.

12. On January 23, 2019, **SHADE** was released on bond pending further charges. On January 28, 2019, **SHADE** turned himself in on an active Felonious Assault warrant filed by Cambridge Police. During the booking process of **SHADE**, he had on his person a cellphone, which was then seized by Cambridge Police Department.

13. **SHADE** is a prohibited possessor of firearms or ammunition based on his criminal history. Specifically, **SHADE** was convicted of Robbery (F2), in Case No. 99CR000036 in Guernsey County Court of Common Pleas on May 7, 1999 and was sentenced to three years in a correctional facility. **SHADE** was paroled early in March of 2000, but had his parole revoked in January 2001 and was re-institutionalized until November 2003. **SHADE** was convicted of Vandalism (F5), in case No. CR2007-0004 in Muskingum County Court of Common Pleas on March 26, 2008 and was sentenced to six months in a correctional facility. **SHADE's** criminal history also includes convictions for misdemeanor charges related to violations of protection orders, assault, thefts, operating a vehicle while intoxicated and falsification.

14. On February 4, 2019, I received and reviewed the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") report from Special Agent Jason R. Burns, who is known to me to be an interstate nexus expert. SA Burns' report confirmed the following regarding the ammunition found:

- CCI/Speer manufactured the *FC*, 9mm LUGER cartridge casings in the state of Idaho for Federal Cartridge Company.

- Federal Cartridge Company assembled/distributed the *FC*, 9mm LUGER ammunition from the State of **Minnesota**.

The information provided by SA Burns indicates that the ammunition traveled interstate commerce.

15. On March 2, 2019, Customs and Border Patrol (CBP) encountered **SHADE** at the U.S. Border/Ambassador Bridge between Detroit, Michigan and Windsor, Canada. During the encounter, and pursuant to CBP's authority, information on his cell phone (614-670-3089) Model LG-H910, serial number 702KPMZ159723, was searched and seized. FBI/JTTF was later notified of this encounter and the results of the search passed to FBI Cincinnati.

16. The following texts were found as relevant to **SHADE'S** status as a prohibited possessor of firearms and ammunition:

- On August 21, 2018, Line #6377 is from **SHADE'S** phone to 210-912-9965, listed in his contacts as an individual with the initials C.B. The text from **SHADE'S** phone reads, "Absolutely I will. I will literally have a staple gun and a baseball bat attached to my hip. Handgun, long gun. Duh"
- On October 23, 2018, Lines #5390 to #5394 are from **SHADE'S** phone to 740-255-6766, listed in his contacts as "Dori," believed by agents to be **SHADE'S** stepmother. The texts from **SHADE'S** phone read, "Yes. Didn't want to transport it back home with the boys in the car. I'll grab it next time I'm down there. Sorry." "You're welcome to take it out back for some stress relief if ya want" "Don't lie. Tell him about it. It's no big deal. I just didn't want him to worry or question why I had it." "Glock19 is probably the most reliable and easy to use. It

has great balance, minimal trigger weight and largest capacity magazine for a 9mm. Plus the ammo is cheaper than other gauge Glocks. You're more than welcome to try that one out. Set up a target low to the ground out near the back treeline." "Okie dokie. I just didn't want you to feel like it was some kinda secret lol."

- On October 29, 2018, Line #5186 is from **SHADE'S** phone to 740-255-6766, listed in his contacts as "Dori". The text from **SHADE'S** phone reads, "I grabbed that glock btw. In case you go to look and it's gone"
- On November 13, 2018, Lines #4947 to #4950 are from **SHADE'S** phone to and from 740-584-1911, listed in his contacts as "Burley." The text exchange reads,
 - **SHADE** "Hey man. Got a firearm question for ya..."
 - Burley "Shoot. Lol"
 - **SHADE** "Glock19. Took it out to a range yesterday to let my friend and her 14 year old daughter get a few shots in. Neither one had ever fired a handgun before. And I'm a still a complete amateur myself lol. Probably not the most ideal teacher. But it was just a little recreation. Full safety with goggles and me doing all loading, chambering, etc" "'Question is... Almost every round the young one fired it jammed. The casing didn't eject. Slide was stuck halfway back. Then I would clear it, rechamber and fire with no problem. Any ideas"
- On January 18, 2019, Lines #1926, #1927 and #1930 from **SHADE'S** phone to and from 740-421-0640, listed in his contacts as an individual with the initials A.B., read,
 - **SHADE** "Wanna go shoot later?"
 - A.B. "Shoot what?"

○ **SHADE** “At the range”

17. Based on my training and experience, I know that the type of ammunition purchased by and later found in **SHADE’S** vehicle in January of 2019 during the Cambridge Police Department search referenced above, is the same type of 9mm ammunition that would be used in a Glock 19, which **SHADE** referenced in the text messages above.

18. The PREMESIS was purchased by **SHADE** on April 8, 2015 and recorded at the county recorder. **SHADE’S** registered and licensed vehicle has been seen on multiple occasions in the driveway of the PREMESIS – even as recent as February 2019. On May 20, 2018, Deputies from the Licking County Sheriff’s Office were dispatched to the PREMESIS and interacted with **SHADE** after an accidental 911 call. On or about June 28 and 29, 2018, USSS agents also attempted to make contact with **SHADE** at the PREMESIS following **SHADE’S** removal from an event where the Vice President of the United States was speaking. After the attempted contact, surveillance photographs (using equipment at the PREMISES) of the USSS agents at the PREMESIS were posted on the social media account of **SHADE**. Based on my training and experience, as well as the text messages referenced above detailing **SHADE’S** apparent ownership and transporting of a Glock 19, I submit there is probable cause to believe that a firearm or evidence of firearm possession would be located at **SHADE’S** residence. Based on my training and experience, it is common for individuals who possess firearms or ammunition to keep such items at their place of residence.

19. Based on my training and experience, I also know that individuals who purchase or own firearms will use electronic devices, such as cellphones or computers, to research purchases, styles and brands of the firearm itself, as well as the types, caliber and brand of ammunition.

Evidence at the Residence

Molotov Cocktails

20. On March 22, 2019, law enforcement executed a search warrant at the PREMISES. During the search of the attached garage, law enforcement located an open box on a work bench containing over a dozen glass jars of different sizes with metal lids. Most of the lids had a small hole drilled in the center. The jars contained pink Styrofoam pieces. Additionally, there were gas cans found on the back porch of the residence.

21. By way of background, on SHADE's cellular telephone that was in his possession on March 2, 2019 when stopped by CBP, there was a list titled "Napalm Mollie" and it set forth the following items: glass jar, 50% Styrofoam, 25% fuel, 25% moth balls.

22. Based on my training and experience, the items at SHADE's residence are indicative of a Molotov cocktail or napalm bomb, which is an explosive/incendiary device. It appears that the holes were drilled in the lids to allow for a wick to be inserted, which would allow the device to be lit on the outside before placing/throwing the object. Possession of these devices is prohibited under 26 U.S.C. § 5861(d) as explosive, incendiary devices are considered destructive devices and destructive devices are considered within the definition of a firearm, pursuant to 26 U.S.C. § 5845(a) and (f).

USSS Tweets

23. On June 15, 2018, the VPOTUS appeared for an event in Columbus, Ohio at the Renaissance Hotel. During the event, Shade entered the venue and was observed standing with a group of protesters wearing a "PRESS" pass that was not familiar to Columbus Police Department (CPD). When approached by CPD officers, Shade was verbally aggressive and subsequently asked to leave the venue. Accordingly, Shade was trespassed from the venue by hotel staff; CPD and

the United States Secret Service (USSS) attempted to interview Shade about the PRESS pass, but were unsuccessful.

24. As a result of Shade's conduct at the event, USSS Special Agent Bart Tackett was assigned to locate and interview Shade. On June 28, 2018, SA Tackett went to Shade's residence, as is listed on his Ohio drivers' license. SA Tackett knocked, but there was no answer. He left a USSS business card, which listed his name and contact information.

25. On June 29, 2018, W.H., an attorney from Michigan, contacted SA Tackett by telephone. W.H. previously represented Shade in another criminal matter in Detroit, Michigan. W.H. inquired as to why SA Tackett had left a business card in Shade's doorway. SA Tackett said he was assigned to follow up and interview Shade based on his trespass at the VPOTUS event. W.H., who no longer represented Shade, indicated that he did not believe Shade would speak with SA Tackett. No further contact was made with Shade.

26. On July 18, 2018, the First Lady of the United States (FLOTUS) tweeted out her gratitude to the USSS and offered condolences to the family of a recently deceased USSS Special Agent. On that same date, as seen below, there was a tweet posted using the Junto Unsilenced Twitter handle, which replied directly to FLOTUS, the USSS (@SecretService) and the President of the United States (POTUS). This tweet directly inquired whether the FLOTUS would say the same for Agent Bart Tackett, which SA Tackett perceived to be a threat to his life inquiring as to whether FLOTUS would also offer condolences to his family. A threat to law enforcement in the performance of the official duties would be a violation of 18 U.S.C. § 115(a)(1)(B).

27. The Twitter account of @JuntoUnsilenced was created on April 20, 2017 with a 614 area code phone number ending in 3089. This telephone number has been registered to Shade since as early as August of 2013.

28. During the execution of the search warrant of **SHADE's** residence, agents found a document on the kitchen table that appeared to be a flyer requesting a phone call if the individual receiving the flyer had been contacted by Bart Tackett. The date on the flyer is July 10, 2018 – eight days before the Tweet referenced above. The name requesting the information was Junto Maquis. I know that one of **SHADE's** Facebook monikers is JWMaquis and submit that Junto refers to Junto Unsilenced, which is a political extremist group to which **SHADE** is affiliated.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a cellular telephone, computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. *Probable cause.* I submit that if a cellular telephone, computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that cellular telephone, computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the

United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data

typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

33. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly

examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

35. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

A handwritten signature in black ink, consisting of a large, stylized 'J' followed by a horizontal line and a small flourish.

Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me
on March 22, 2019:

A handwritten signature in blue ink, appearing to be 'Elizabeth Preston Deavers'.

~~ELIZABETH PRESTON DEEVERS~~ N. M. 14NY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is **212 Harborview Drive, Thornville, Ohio 43076**, further described as being lot # 11 in Harborview Heights subdivision. The property was purchased by John William Shade, III on April 8, 2015 and recorded at the county recorder. It is a single family, split level dwelling with light blue siding and stone exterior. The numbers "212" appear on the mail box next to the driveway.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 922(g)(1), 26 U.S.C. § 5861(d) and 18 U.S.C. § 115(B), those violations involving **SHADE** and occurring after June 28, 2018, including:
 - a. Information and records, to include any communications, photographs or documents, related to the purchase, possession, use, storage, transportation, transfer or sale of Firearms or ammunition;
 - b. Records and information relating to potential witnesses that may have observed **SHADE** in possession of a firearm or ammunition, such as at a range;
 - c. Records and information, as well as any physical items, that involve the research, possession, use, transfer, purchase, manufacture or sale of items used in making Molotov cocktails or other explosive, improvised or incendiary devices; and
 - d. Records and information that involve U.S. Secret Service, to include but not limited to Special Agent Bart Tackett and any research, plan, effort, solicitation or otherwise of threats, harassment or violence towards law enforcement officers.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review any information removed from **212 Harborview Drive, Thornville, Ohio 43076** in order to locate the things particularly described in this Warrant.